



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/014,747	10/26/2001	William H. Dixon	210818	5741

22971 7590 10/18/2005
MICROSOFT CORPORATION
ATTN: PATENT GROUP DOCKETING DEPARTMENT
ONE MICROSOFT WAY
REDMOND, WA 98052-6399

EXAMINER

DERWICH, KRISTIN M

ART UNIT PAPER NUMBER

2132

DATE MAILED: 10/18/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

DETAILED ACTION

Response to Amendment

1. This action is in response to amendments received August 1, 2005.

Response to Arguments

2. Applicant's arguments filed August 1, 2005 have been fully considered but they are not persuasive. With regard to Applicant's argument that Nessel does not teach "an access control component for providing purpose authorization for authenticated users based on rules in a connection policy associating users with purposes", Examiner respectfully disagrees. The filtering rules function as purpose authorizations since the traffic that goes through the connection must adhere to the filtering rules applied and therefore must be authorized in order to proceed. The user is authenticated at the onset of the connection (12:9-13), then the filtering rules that make up the connection policy are applied. Thus, the filtering rules function as purpose authorizations since, after the user has been authenticated to make a connection, then all traffic the user sends is subject to be the filtering rules, therefore, it must all be authorized from the authenticated user before going through.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

Art Unit: 2132

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Hereafter patent literature that is referenced as prior art will be cited by column and line number in the form of (column number:line number range). For example, the citation (6:23-27) refers to lines 23-27 of the 6th column in the reference.

1. Claims 1, 5, 7-12 rejected under 35 U.S.C. 102(b) as being anticipated by Nessel et al. (Nessel), U.S. Patent No. 5,968,176.

As per claim 1:

Nessel discloses a distributed firewall (DFW) for use on an end system, comprising:

an authentication component for providing user authentication for connection attempts from users attempting to access the end system via a network (13:39-45);

In this instance the switch functions as an authentication component by providing user authentication protocols for servers, wherein servers function as networks, attempting to access an end system.

an access control component for providing purpose authorization for authenticated users based on rules in a connection policy associating users with purposes (12:10-11, 17-19; 16:6-10);

Wherein the NIC or modem functions as the access control component and the filtering rules function as the connection policy associating users with specific filtering rules which function as purpose authorizations.

an enforcement component for enforcing the connection policy rule for the authenticated user from whom the traffic is sent as the traffic is received (16:10-12);

Art Unit: 2132

Wherein the enforcement component is the Access Server.

and wherein the authentication component utilizes an aggregate of the users in the connection policy to authenticate users (16:58-67 – 17:1-3).

As per claim 5:

Nessett discloses a DFW wherein the enforcement component utilizes Internet protocol security (IPSec) protocol to maintain security of communications from the authenticated user when the communications are within the rule in the connection policy (16:27-29).

As per claim 7:

Nessett discloses a DFW further comprising an inspection component for inspecting packets from an authenticated user (13:53-56).

Wherein the router functions as the inspection component and checking the packet's quality of service, security option data and hop count function as inspecting the packet.

As per claim 8:

Nessett discloses a DFW wherein the connection policy is defined in a pluggable policy component (16:6-12).

Wherein the Access Server functions as a pluggable policy component.

As per claim 9:

Nessett discloses a DFW wherein the pluggable policy component is downloaded from a centralized administrative policy (15:29-33).

Art Unit: 2132

Wherein the centralized administrative policy is the Remote PSTN and Remote Access Router.

As per claim 10:

Nessett discloses a DFW wherein the pluggable policy component is modifiable on the end system (17:12-14).

Wherein the Remote Access equipment includes the Access Server which functions as the pluggable policy component.

As per claim 11:

Nessett discloses a DFW further comprising an access control component through which the connection policy may be defined (7:36-38).

As per claim 12:

Nessett discloses a DFW further comprising an access control component having a user interface (UI) through which the connection policy is defined (7:38-41).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

2. Claims 2-4 rejected under 35 U.S.C. 103(a) as being unpatentable over Nessett (U.S. 5,968,176) as applied to claim 1 above and further in view of Harkins et al. (RFC 2409, The Internet Key Exchange) hereinafter referred to as Harkins.

Art Unit: 2132

As per claim 2:

Nessett teaches an authentication component utilizing IPSEC to authenticate users based on the aggregate of users in the connection policy but fails to teach users being authenticated in IKE main mode as the IPSEC protocol. However, Harkins discloses utilizing IKE in main mode to authenticate users (pg. 20, section 8, 3rd paragraph, lines 1-2). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to use IKE main mode in order to authenticate a user because this provides for perfect forward secrecy of keys and identities which would allow for better security (pg. 20, section 8, 1st and 2nd paragraph).

As per claim 3:

Nessett teaches an authentication component utilizing the rule in the connection policy to authenticate the user but fails to teach the authentication in IKE quick mode. However, Harkins discloses utilizing IKE quick mode to complete the authentication of a user (pg. 20, section 8, 4th paragraph, lines 1-2). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to complete authentication in IKE quick mode because this would have provided for perfect forward secrecy of the keys and identities which would provide better security (pg. 20, section 8, 1st and 2nd paragraph).

As per claim 4:

Nessett fails to teach an authentication component that transmits a secure notify message to the authenticated user when the user sends traffic in quick mode that exceeds an authority governed by the rule in the connection policy associated with the

Art Unit: 2132

user. However, Harkins discloses a notify message being sent when identifiers are not acceptable based on the policy established by the client (pg. 13, 4th paragraph, lines 6-10). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to notify the user when identities exceed the policies set forth because the ensures traffic is directed to the correct tunnels when multiple tunnels exist (pg. 13, 5th paragraph, lines 1-4).

3. Claim 6 rejected under 35 U.S.C. 103(a) as being unpatentable over Nessett (U.S. 5,968,176) as applied to claim 1 above and further in view of LeBlanc (Bind Basics).

As per claim 6:

Nessett fails to teach enabling IPsec on a socket and binding it in exclusive mode. However, LeBlanc discloses a method for binding the socket in exclusive mode using `SO_EXCLUSIVEADDRUSE` (pg. 2, 6th paragraph, lines 1-2). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to enable IPsec on a socket binding in exclusive mode because the operating system prefers a socket bound to a specific address since this will also prevent hijacker attacks (pg. 2, 2nd paragraph, lines 2-6).

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Kristin Derwich whose telephone number is 571-272-7958. The examiner can normally be reached on Monday - Friday, 8:00-5:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

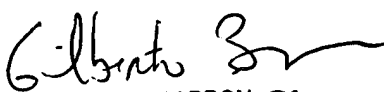
Kristin Derwich

Application/Control Number: 10/014,747
Art Unit: 2132

Page 9


KMD

Examiner
Art Unit 2132


GILBERTO BARRON JR.
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100